iconectiv

Louise L M Tucker
VP Regulatory and Senior Counsel
m 202.368.5180
ltucker@iconectiv.com | iconectiv.com

October 20, 2016

Ex Parte
Via Electronic Submission

Marlene H. Dortch
Secretary
Federal Communications Commission
445 Twelfth Street, S.W.
Washington, DC 20554

Re: *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106

Dear Ms. Dortch:

On October 18, 2016 Chris Drake, Suresh Subramanian and Louise Tucker of iconectiv, and Maria Kirby of CTIA met by telephone with Nick Degani of Commissioner Ajit Pai's office, and on October 19, we met by telephone with Melissa Kirkel and Sherwin Siy of the Wireline Communications Bureau, Charles Mathias and Alison Nemeth of the Wireless Telecommunications Bureau and Nicole McGinnis of the Public Safety and Homeland Security Bureau. The purpose of both calls was to discuss the issues presented in iconectiv's Comments and Reply Comments in this proceeding[1] and our October 13, 2016 letter filing in the above-referenced docket.

During both calls, iconectiv repeated our support for the permissionless use and sharing of CPNI and CPI as articulated in the Commission's privacy proceeding for the purposes of mobile identity fraud prevention. Timely detection and prevention of account take over fraud requires an identity verification process in which a trusted third party identity partner, can aggregate relevant customer data across networks in advance of a security incident. When anomalous use of service behavior is detected, such as involving the change of a device associated with the telephone number, the third party, without transferring any customer data, can protect the consumer by notifying the financial institution, healthcare provider or other

[1] Comments and Reply Comments of Technologies, Inc, d/b/a iconectiv, WC Docket No. 16-106 (filed May 27 and July 19, 2016).

company to be alert and prevent possible fraud or disclosure of confidential information.

Typical authentication methods involving “something you know”, like passwords and knowledge challenges, are easily procured by fraudsters. “Something you have” or “something you are” such as hard tokens, and biometrics are not ubiquitous enough to protect the majority of consumers. The telephone is the primary authenticator representing “something you have” that can reach the vast majority of the consumer base to provide multi-factor authentication in our digital economy. However, the phone number must then be safeguarded from account take over so it cannot be used to perpetrate fraud and other consumer harms. Access to cross network information is key to mitigating this vulnerability.

Accordingly, to eliminate ambiguity and enable much greater protection for consumers, we explained that the Commission's regulations should clarify that BIAS providers and traditional communication service providers (CSPs) may share or disclose customer CPNI, CPNI pursuant to Section 222(d) with a third party without prior customer consent provided that the third party uses the protected data only for the purposes of fraud prevention and response. Absent such clarification from the Commission, however, BIAS providers and traditional CSPs may continue to be cautious about how and when they can share or disclose data covered by Section 222 and consumers will continue to suffer the harms enabled by account takeover as they do today.

If additional information is needed, please do not hesitate to reach out to me or my colleagues.

One electronic copy of this Notice is being submitted in the above-referenced proceeding in accordance with Section 1.1206 of the Commission’s rules.

Respectfully submitted,

Louise L M Tucker